Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (previously presented) A method of digitally signing a message exchanged between a pair of correspondents in a data transmission system, one of said pair of correspondents being the signer and having a private key and a public key derived from the private key and available to the other of said pair of correspondents, said method comprising the steps of subdividing said message into a pair of bit strings, utilizing one of said bit strings to compute a first signature component, forming from said first signature component and another of said bit strings an intermediate signature component, utilizing said intermediate component and said private key to provide a second signature component and combining said first and second components with said other of said bit strings to provide a signature.

2. (previously presented) A method according to claim 1 wherein redundancy in said one of said bit strings is compared to a predetermined level prior to computing said first signature component.

3. (previously presented) A method according to claim 2 wherein said redundancy is adjusted to exceed said predetermined level.

4. (currently amended) A method according to claim 3 wherein data is added to said one of said [one] bit strings to adjust said redundancy.

5. (currently amended) A method according to claim 4 wherein an indicator is included in said one of said bit strings to indicate the data added.

6. (previously presented) A method according to claim 1 wherein said second component is generated by hashing said first component and said other bit string.

7. (currently amended) A method of verifying a message subdivided into a pair of bit strings from a signature of a purported signer including at least one component having only one of said bit strings encrypted therein, and the other of said bit strings, said purported signer having a private key used in the computation of said signature and a corresponding public key available for use in verification, said method comprising the steps of combining said one component with the other of said bit strings, recovering said one of said bit strings from said combination using publicly available information of the purported signer including said public key and examining said recovered one of said bit strings for a predetermined characteristic.

8.(currently amended) A method according to claim 7 wherein said combination of said one component and said other bit string includes hashing a combination of said one component and said other of said bit strings.

9. (previously presented) A method according to claim 8 wherein said predetermined characteristic is the redundancy of said recovered one bit string.

10. (currently amended) A method according to claim 9 wherein said signature includes a second component derived from a combination of said one component and said other of said bit strings and said one of said bit strings, is recovered utilising said second component.

11. (new) A method according to claim 1 wherein said first signature component is formed by applying a function to said one of said bit strings and said one of said bit strings may be recovered from said signature component by applying a complementary function to said signature component.

12. (new) A method according to claim 11 wherein said function is encryption with a key, said key is recoverable from said signature, and said complementary function is decryption with said key.

13. (new) A method according to claim 12, wherein said key is a short-term public key derived

a2

from a short-term private key used in the provision of said second signature component.